

WHAT IS CLAIMED IS:

1. A method comprising:
 - 5 designating a location in a directory server;
 - providing attribute-related data comprising a filter expression; and
 - selectively controlling access to an entry situated at the designated location using
 - 10 the filter expression in said attribute-related data.
2. The method of claim 1, wherein the filter expression is selectively associated with a class of operations.
- 15 3. The method of claim 2, wherein the filter expression is associated with a class of operations selected from a predefined group comprising “add” and “delete” classes of operations.
4. The method of claim 3, wherein the predefined group further comprises the
- 20 “search” class of operations.
5. The method of claim 1, wherein the filter expression is selectively associated with an attribute.
- 25 6. The method of claim 1, wherein said selectively controlling comprises denying access to the entry if the filter expression refers to more than one attribute type.
7. The method of claim 1, wherein said selectively controlling is repeated for each
- attribute value of an attribute type being referred to in the filter expression.

30

8. The method of claim 1, wherein said providing comprises providing data adapted to designate attribute values in the form of a plurality of filter expressions, defined in accordance with a predefined syntax.

5 9. The method of claim 8, wherein the plurality of filter expressions are interconnectable by an AND condition.

10. A directory server request processor comprising:

10 a filter execution processor configured to generate a result of a filter expression;
and

an access control instruction processor comprising an interpreter, wherein the
interpreter calls the filter execution processor in response to a filter-
15 indicating keyword in an access control instruction and controls access
through the directory server request in accordance with the result of the
filter execution processor.

11. The access control instruction processor of claim 10, wherein the interpreter is
20 capable of repetitive operation for processing a plurality of interconnected filter
expressions.

12. The access control instruction processor of claim 10, wherein the interpreter
further comprises a filter interpreter for determining whether a filter expression refers to
25 more than one attribute type.

13. The access control instruction processor of claim 10, wherein the interpreter is
capable of at least partially repetitive operation for processing each attribute value of an
attribute type being referred to in the filter expression.

30

14. A computer readable medium comprising program instructions computer executable to:

receive a request to access an attribute of a directory server entry;

5

deny access if a criterion defined by a filter expression associated with the attribute is not met by a first value of the attribute.

15. The computer readable medium of claim 14, wherein the program instructions are computer executable to authorize access if the criterion defined by the filter expression associated with the attribute is met by each value of the attribute.

16. The computer readable medium of claim 14, wherein the request to access comprises a request to delete the first value of the attribute and wherein the filter expression is associated with operations that delete values of the attribute.

17. The computer readable medium of claim 16, wherein the criterion defined by the filter expression specifies that the attribute cannot be deleted if a value of the attribute is the first value.

20

18. The computer readable medium of claim 14, wherein the request to access comprises a request to add the first value of the attribute and wherein the filter expression is associated with operations that add values of the attribute.

19. The computer readable medium of claim 18, wherein the criterion defined by the filter expression specifies that the attribute cannot be added if a value of the attribute is the first value.

20. The computer readable medium of claim 1, wherein the program instructions are computer executable to evaluate the filter expression for each instance of the attribute and

deny access if any instance of the attribute fails to satisfy the criterion defined by the filter expression.

21. A method comprising:

5

receiving a request to access an attribute of a directory server entry;

denying access if a criterion defined by a filter expression associated with the attribute is not met by a first value of the attribute.

10

22. The method of claim 21, further comprising authorizing access if the criterion defined by the filter expression associated with the attribute is met by each value of the attribute.

15

23. The method of claim 21, wherein the request to access comprises a request to delete the first value of the attribute and wherein the filter expression is associated with operations that delete values of the attribute.

20

24. The method of claim 23, wherein the criterion defined by the filter expression specifies that the attribute cannot be deleted if a value of the attribute to be deleted is the first value.

25

25. The method of claim 21, wherein the request to access comprises a request to add the first value of the attribute and wherein the filter expression is associated with operations that add values of the attribute.

30

26. The method of claim 25, wherein the criterion defined by the filter expression specifies that the attribute cannot be added if a value of the attribute to be added is the first value.

27. The method of claim 21, further comprising evaluating the filter expression for each instance of the attribute and denying access if any instance of the attribute fails to satisfy the criterion defined by the filter expression.

5 28. A directory server comprising:

an access control processor for processing an access control instruction
controlling access to a first attribute of a first entry, wherein the access
control instruction specifies a filter expression; and

10

a filter processor for generating a result of a filter expression for a first value of
the first attribute;

15

wherein the access control processor provides the filter processor with the filter
expression and the first value and controls access to the first attribute of
the first entry based on the result of the filter expression;

wherein the filter expression defines a criterion for values of the first attribute.

20 29. The directory server of claim 28, wherein the result of the filter expression is false
if the first value of the first attribute fails to meet the criterion defined in the filter
expression.

25 30. The directory server of claim 28, wherein the access control processor provides
the filter processor with the filter expression and the first value if a requested access to
the first attribute involves a class of operations associated with the filter expression.

31. The directory server of claim 28, wherein the result of the filter expression is false
if any value of the first attribute fails to meet the criterion defined in the filter expression.

30